

(10)



Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number:

0 172 439
B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: 12.07.89

(51) Int. Cl.⁴: **G 11 B 23/28**

(71) Application number: **85109334.4**

(22) Date of filing: 25.07.85

(54) Copy protected disk.

(30) Priority: 13.08.84 US 639733

(43) Date of publication of application:
26.02.86 Bulletin 86/09

(45) Publication of the grant of the patent:
12.07.89 Bulletin 89/28

(84) Designated Contracting States:
DE FR GB

(50) References cited:
EP-A-0 021 971
FR-A-2 535 885
GB-A-2 055 501
GB-A-2 113 432
US-A-4 086 634

(70) Proprietor: **VERBATIM CORPORATION**
323 Soquel Way
Sunnyvale California 94086 (US)

(72) Inventor: **Bond, Charles R.**
502 Sark Court
Milpitas, CA 95035 (US)

(74) Representative: **Parent, Yves**
Kodak-Pathé Département Brevets et Licences
CRT 60/1 -Zone Industrielle
F-71102 Chalon-sur-Saône Cédex (FR)

EP 0 172 439 B1

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European patent convention).

Courier Press, Leamington Spa, England.

Description

Field of the Invention

The present invention relates generally to magnetic disk data storage media and more particularly to disk data storage media which contain uncopyable sequences of encoded data.

Description of the Prior Art

Personal or microcomputers are increasingly employed in a variety of applications in the home, business, scientific and educational environments. Typically, such computers store data on and retrieve data from disk storage media. Flexible disk storage media are most commonly used in conjunction with such microcomputers, although hard disk media may be employed as well. Designing, manufacturing and marketing of applications software, written onto such disks, is a major industry, accounting for millions of dollars in sales annually. Manufacturers expend substantial sums of money on the development of such programs, often only to see them copied by unauthorized "pirates". Further, particular disks produced in-house containing proprietary, confidential or otherwise sensitive information may require copy protection and/or permanent identification.

Various means of protecting and/or identifying certain types of information stored on various types of storage media are known in the art. However, these means are generally complex and require special equipment or are not adaptable to flexible data storage disks, or both. U.S. Patent 4,333,113 issued to *Kalinowski* describes a method for monitoring the reproduction of sound or audiovisual recordings by coding auxiliary information in a limited frequency range and superimposing it on the primary information. This method does not actually protect against copying the master because the master having the auxiliary information can be copied using ordinary duplication techniques. U.S. Patent 4,325,089 issued to *Ito* describes a method for safeguarding data which is merely a means of magnetically destroying the data upon attempts to gain unauthorized access. Such device has limited use as the data becomes unreadable to the intended user, as well as the unauthorized user, and requires that the data be maintained within the apparatus of the invention.

U.S. Patents 4,086,634 and 4,040,099 issued to *Cook* both relate to a method and apparatus for detecting tape piracy by preparing the program source material to include preselected inaudible signals to indicate the origin of the material in a manner similar to *Kalinowski* or to produce unacceptable interference signals to spoil the copy. U.S. Patent 3,551,608 issued to *Balint* describes a method and apparatus for recording a plurality of copies from a master audio sound track, and for checking the quality of the copies relative to the master.

U.S. Patent 3,004,104 issued to *Hembrooke* discloses a method and apparatus for the identifi-

cation of signals, in order to positively identify the origin thereof. *Hembrooke*, like much of the art, relies on encoding an inaudible signal in a narrow frequency band. U.K. Patent Application 2,055,501A, submitted by *Edmunds* discloses an apparatus specifically for the purpose of producing video tapes which cannot be copied on an ordinary video tape recorder.

Other methods to copyproof disks currently known in the art include the use of weak signal pulses to interfere with the nominal transitions encoded onto a data track. Such a technique has been disclosed by an article appearing in *Electronics*, September 22, 1983, entitled "Disk-Drive Generated Pulses Foil Piracy". This technique requires special equipment to generate the weak pulses, and may not operate at all when used on a drive with automatic gain control. Attempts have been made to provide a disk with a permanent serial number for positive identification by using high-coercivity media and special recording apparatus. These have been unsuccessful thus far.

In view of the prior art, there remains a need for a method of electronically identifying magnetic data storage media, and for providing a simple, positive means to differentiate a copy of the data from the original whereby valuable information stored on the media may be safeguarded.

Summary of the Present Invention

It is therefore an object of the present invention to provide an improved data storage disk which contains a tamper resistant serial number.

It is a further object of the present invention to provide a copy-protected data storage disk which, if copied, will produce a copy having a detectable signature.

It is a further object of the present invention to produce a tamper resistant and copy-protected data storage medium which may be produced with existing recording and duplication equipment.

It is a further object of the present invention to provide a tamper resistant and copy-protected data storage medium which does not require drive modification.

It is a further object of the present invention to provide a tamper resistant and copy-protected data storage medium which is not susceptible to failure when used on a drive with automatic gain control.

Briefly, a preferred embodiment of the present invention includes a flexible magnetic data storage disk having at least one specially encoded data pattern comprising a "burst" located in at least one disk sector. This code burst comprises a nonstandard recording pattern which is designed to differ from the nominal transitions usually present on a data track and to interfere with normal reading of the data. Without the nominal transitions, the read electronics "drifts" and interprets the code burst as a random series of ones and zeros. To verify the status of the disk as an original, the sector containing the code burst is

read twice, and the data generated therefrom is compared. The original disk will produce random data each time the burst is read, thus the resultant data will be dissimilar. A copy however will, on successive readings, produce the same data from the sector containing the code burst. This result follows from the nature of the duplicating process wherein the copy is produced by reading the original and writing the copy therefrom. The code burst will thus be interpreted and fixed on the copy such that each time the copy is read, the same data will be produced.

For certain security applications, a serial number may be encoded onto the disk immediately following the code burst. The serial number will be tamper resistant because any attempt to rewrite the number will necessarily erase the code burst. Thus, a check for the presence of the code burst will automatically verify the integrity of the serial number.

It is an advantage of the present invention that a data storage disk may be produced carrying a tamper resistant serial number.

It is another advantage of the present invention that a data storage medium may be produced having a data signature which cannot be copied.

It is another advantage of the present invention that the data storage disk may be produced using standard recording and duplication equipment.

It is another advantage of the present invention that no modification of a disk drive is necessary to verify the data patterns.

It is another advantage of the present invention that the data storage disk may be used with drives having automatic gain control without loss of the code bursts.

The present invention will become apparent after having read the following detailed description of the preferred embodiment as illustrated by the various drawing figures.

In the Drawing

Fig. 1 is a top view of a flexible magnetic recording disk of the present invention;

Fig. 2 is a schematic graphical representation of a sector of the disk of the present invention;

Fig. 3 is a schematic showing coding and clocking information; and

Fig. 4 is a schematic logic circuit used to achieve the code bursts of the present invention.

Detailed Description of the Preferred Embodiment

Fig. 1 illustrates a flexible data storage disk of the present invention and referred to by the general reference character 10. The disk 10 includes a central mounting aperture 12 which is coaxial with a disk central axis 13. A plurality of data tracks 14 are concentrically arrayed about the disk 10 coaxial with the axis 13. Typically there are forty data tracks 14 although there may be any lesser number of data tracks 14 and there can be a greater number to some extent, depending on the desired track density. The disk 10 may further be divided into a plurality of sectors 16 which are bounded about two sides thereof by concentric

circular lines and about an additional two sides by radial lines projecting from the axis 13. The disk 10 is divided into sixteen sectors but this number can vary, for example, ten, twelve, twenty-four or thirty-six sectors are commonly used in the art, and all are consistent with the present invention. The tracks 14 and sectors 16 are schematically illustrated in Fig. 1, which also illustrates a read/write head 20 positioned over the disk 10.

Fig. 2 illustrates in schematic view, a portion of an individual sector 16, with the data track 14 represented as a continuous address header 30 followed by a gap 32, a data sync gap 34, a data field 36 and an epilog 38.

Near the beginning of the data field 36 is a code burst 40 which comprises a series of encoded information, approximately twenty bytes long, which differs from the nominal transitions normally present in encoded information. The code burst 40 is a "hard" bit recorded at normal signal strength, nevertheless, it is adapted to produce patterns that are beyond the ability of a disk controller chip 44, illustrated schematically in Fig. 1, to recover accurately. Thus, each time the code burst 40 is read by the read/write head 20, the magnetic impulses generated by the controller chip 44 differ from the impulses generated by a previous reading. Any attempts to copy the disk 10 will copy the code burst 40 as interpreted by the duplicating equipment used to make the copy. The data resulting from a copy of the code burst 40 will thus be fixed, and will so remain each time the copy is read. This provides a secure read-only signature to distinguish the original disk 10 from a copy thereof. The data on data field 36 cannot be written over without also writing over and destroying the code burst 40 because all of the disk controller chips 44 presently employed are limited to writing only, once switched to the write mode. Thus, by twice reading and comparing the recovered data, the disk 10 can be verified as an original.

The code burst 40 is generated by encoding in such a way as to interfere with the nominal transitions occurring on a data track 14. Various methods may be employed to do this. In the disk 10 the code burst 40 is generated by altering a clock frequency to be much higher or much lower than normal to eliminate the normal sequence of transitions which is interpreted by the controller chip 44 as a binary sequence of ones and zeros.

Fig. 3 is a schematic time chart showing (a) a normal series of uniformly spaced clock pulses, (b) a long-duration clock pulse for a code burst 40 of the present invention, and (c) a series of short duration clock pulses for a burst 40 of the present invention.

Fig. 4 is a schematic circuit diagram designed to produce the code burst 40 clock pulse of Fig. 3b. Processing events taking place within the computer are controlled by a clock signal, comprising a sequence of regular, periodic pulses or transitions, as illustrated in Fig. 3a. These clock pulses may be physically written adjacent to a series of data pulses, or if a self-clocking code is used, the

clock pulses are written within the data pulses, and special coding rules are employed to differentiate the two. The circuit of Fig. 4 includes a first clock 45 for generating a normal series of transitions, and a second clock 46 having a frequency of, for example, one tenth that of clock 45, for generating the code burst 40. The output of each clock 45 and 46 is coupled to a first AND gate 47 and a second AND gate 48, respectively. One AND gate, for example AND gate 47 has a clock enabling signal 50 coupled to its other input. The other AND gate, for example, AND gate 48 has coupled to its other input an inverse clock enabling signal 52. The signals 50 and 52 are generated by appropriate software (not shown) and are complementary to each other such that when one AND gate is enabled, the other is disabled. The outputs of the AND gate 47 and AND gate 48 are coupled to an OR gate 54 which is connected in turn to a clock input of an encoder 56. The encoder 56 may be any circuit known in the art for accepting clock and data pulses, and producing a signal therefrom which may be encoded on the disk 10. The output of the encoder 56 controls a write circuit 58 to produce either normal clock pulses or the nonstandard pulses of the code burst 40. This modification of the clocking may be used with both self-clocking and non self-clocking coding schemes.

An alternative method of creating the code burst 40 utilizes a direct current (DC) erase to produce a single, long duration pulse as illustrated in Fig. 3b. Such a pulse is the equivalent of a pulse produced using the clock 46 having a much lower frequency than that of the clock 45.

A number of special data storage applications would greatly benefit from a disk 10 having an indelible serial number encoded within the data tracks 14. Such a disk would be useful in applications demanding some degree of security, for example, in home banking, where a bank's computer needs to verify the particular disk to which it is downloading information. Such a system offers a much greater degree of security than a system employing a password, which is relatively easy to discover. For such applications, a serial number 60, illustrated in Fig. 2, is encoded into the data field following the code burst 40. The serial number may be encoded and written on the disk 10 by any means known in the art, and it is written to closely follow the code burst 40. The presence of the code burst 40 ensures the integrity of the serial number 60 which follows, because rewriting the serial number would necessarily require erasing the code burst 40.

The code burst 40 and serial number 60 may be placed on any one sector or plurality of sectors 16 of the disk 10 depending on the needs of the end user. While multiple code bursts 40 are easily added to the disk 10, a single burst 40 is generally all that is needed to obtain the desired security. The use of multiple bursts 40, however, lends itself to another application. The disk 10 may have, for example, four code bursts 40 located about four different sectors 16. Appropriate soft-

ware (not shown) may be designed for the disk 10 so that each time the disk is run, one of the bursts 40 will be written over. The software includes instructions so that each time the disk 10 is rebooted, it will search for the first random data pattern, and verify it by successive readings. After the disk 10 has been run four times, no code bursts 40 remain, and the software refuses to run. In this instance, the code bursts 40 are being used as "tickets" to allow a predetermined number of runs. Providing the disk 10 with multiple code bursts 40 and utilizing it in combination with the appropriate software would allow businesses engaged in renting disks containing particular applications software to charge by the number of runs, rather than by time.

While the disk 10 has been described in terms of a flexible, or "floppy" disk, it should be noted that the disk of the present invention may be a hard disk as well.

Claims

1. A copy protected magnetic information storage medium comprising:

a substrate having at least one magnetic recording layer suitable for recording in a plurality of data tracks; and characterised by

a code burst having a segment of abnormal transitions comprising a sequence of nonstandard code recorded at nominal signal strength, and adapted to be nonrecoverable by a computer read circuit, the code burst being located on at least one of said data tracks.

2. The magnetic information storage medium of claim 1 wherein,

the code burst comprises a code written by altering a clock frequency to produce clocking signals which are beyond the ability of said read circuit to distinguish.

3. The magnetic information storage medium of claim 2 wherein,

said clock frequency is approximately one tenth of a nominal clock frequency.

4. The magnetic information storage medium of claim 1 wherein,

the code burst comprises a code written by utilizing a direct current erase over a portion of said data track comprising the code burst.

5. The magnetic information storage medium of claim 1, wherein,

the substrate includes a plurality of radially arrayed sectors and the code burst follows a data sync gap in one of said sectors; and

a serial number is encoded about the recording track following the code burst.

6. The magnetic information storage medium of claim 1, and further including,

a plurality of code bursts, located about different portions of the recording tracks, the bursts being adapted for use with a software program designed to sense the presence of the bursts by a random data pattern generated therefrom, the software further being adapted to erase at least one burst each time said program is run, whereby

said bursts act as tickets allowing said program to run only a preselected number of times.

7. The magnetic information storage medium of claim 1 wherein,

said substrate is a flexible disk.

8. A method for producing a flexible magnetic information storage medium, having an uncopyable magnetic signature, characterised by

recording at least one code burst about a recording track of the medium, the code burst having a segment of abnormal transitions and comprising a sequence of nonstandard code which cannot be recovered by a data recovery circuit, said abnormal transitions resulting in random data when read by said circuit.

9. The method of claim 8, wherein, the code burst is produced by altering a normal clock signal.

10. The method of claim 8, wherein, the code burst is produced by generating a direct current erase signal.

11. The method of claim 8, and further including, a serial number encoded following the code burst for positive identification of the medium.

Patentansprüche

1. Kopiergeschütztes magnetisches Informationsspeichermittel bestehend aus einem Träger mit mindestens einer magnetischen Aufzeichnungsschicht, welche eine Vielzahl von Spuren für die Informationsaufzeichnung aufweist, dadurch gekennzeichnet, daß eine Code-Folge aufgezeichnet ist, die einen Abschnitt von anomalen Signalübergängen enthält, der aus einer Folge nichtstandardisierter Codes besteht, welche bei nominaler Signalstärke aufgezeichnet wurden und derart beschaffen sind, daß sie von einer Computerdatabausleseeinrichtung nicht ausgelesen werden können, wobei die Code-Folge in mindestens einer der Spuren enthalten ist.

2. Magnetisches Informationsspeichermittel nach Anspruch 1, dadurch gekennzeichnet, daß die Code-Folge einen durch Verändern einer Taktfrequenz gebildeten Code aufweist, dessen Taktsignale von der Ausleseeinrichtung nicht erkannt werden können und damit nicht auswertbar sind.

3. Magnetisches Informationsspeichermittel nach Anspruch 2, dadurch gekennzeichnet, daß die Taktfrequenz etwa ein Zehntel einer nominalen Taktfrequenz beträgt.

4. Magnetisches Informationsspeichermittel nach Anspruch 1, dadurch gekennzeichnet, daß die Code-Folge einen Code aufweist, der durch Anwendung einer Gleichstrom-Löschung über einem Teil der die Code-Folge aufweisenden Spur gebildet ist.

5. Magnetisches Informationsspeichermittel nach Anspruch 1, dadurch gekennzeichnet, daß der Träger eine Vielzahl von radial angeordneten Sektoren aufweist und die Code-Folge in einem dieser Sektoren einer Datensynchronisationslücke folgt, und daß in die auf die Code-Folge folgenden Aufzeichnungsspur eine Seriennummer codiert ist.

6. Magnetisches Informationsspeichermittel nach Anspruch 1, gekennzeichnet durch eine Vielzahl von an verschiedenen Teilen der Aufzeichnungsspuren befindlichen Code-Folgen, die zur Verwendung mit einem zur Ermittlung der Code-Folgen dienenden Softwareprogramm geeignet sind, wobei das Softwareprogramm das Vorhandensein der Code-Folgen mit Hilfe eines aus diesen abgeleiteten Datenzufallsmusters ermittelt und des weiteren dazu geeignet ist, bei jeder Benutzung mindestens eine der Code-Folgen zu löschen, wobei die Code-Folgen als aufbrauchbare Zugangsberechtigung dienen, so daß das Programm nur für eine zuvor festgelegte Anzahl von Benutzungen verwendbar ist.

7. Magnetisches Informationsspeichermittel nach Anspruch 1, dadurch gekennzeichnet, daß der Träger eine flexible Scheibe ist.

8. Verfahren zur Herstellung eines flexiblen magnetischen Informationsspeichermittels mit einer nicht kopierbaren magnetischen Kennung, dadurch gekennzeichnet, daß man mindestens eine Code-Folge auf einer Spur des Speichermittels aufzeichnet, wobei die Code-Folge einen Abschnitt von anomalen Signalübergängen enthält und aus einer Folge nichtstandardisierter Codes besteht, die von einer Databausleseeinrichtung nicht ausgelesen werden können, wobei die anomalen Übergänge Zufallsdaten ergeben, wenn sie von der genannten Leseinrichtung ausgelesen werden.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Code-Folge durch Verändern eines herkömmlichen Taktsignals erzeugt wird.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Code-Folge durch Erzeugen eines Gleichstrom-Löschsignals zustandekommt.

11. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß zur Identifizierung des Speichermittels nachfolgend auf die Code-Folge eine Seriennummer codiert ist.

Revendications

1. Support magnétique de stockage d'informations protégé contre la copie comprenant un substrat ayant au moins une couche d'enregistrement magnétique adaptée pour enregistrer sur une pluralité de pistes et caractérisé en ce qu'il comprend une clef composée pour partie de transitions différentes de celles utilisées pour le reste des informations et comprenant une pluralité de codes hors-norme enregistrés à un niveau de signal normal et irrécupérables par un dispositif de lecture d'ordinateur, la clef étant disposée sur au moins une desdites pistes.

2. Support magnétique de stockage d'informations selon la revendication 1, dans lequel le clef comprend un code obtenu en modifiant la fréquence d'horloge afin de produire des signaux d'horloge dont la fréquence se situe en dehors de la plage de fréquences d'horloge pouvant être distinguées par le dispositif de lecture.

3. Support magnétique de stockage d'inform-

ations selon la revendication 2, dans lequel ladite fréquence d'horloge est dix fois plus petite que la fréquence d'horloge nominale.

4. Support magnétique de stockage d'informations selon la revendication 1, dans lequel la clef comprend un code réalisé au moyen d'un courant continu d'effacement que l'on applique sur une partie de la piste contenant ladite clef.

5. Support magnétique de stockage d'informations selon la revendication 1, dans lequel le substrat comprend une pluralité de secteurs disposés radialement, la clef étant placée après la zone de synchronisation des données dans l'un des secteurs; et dans lequel un numéro de série relatif à la piste d'enregistrement est écrit après la clef.

6. Support magnétique de stockage d'informations selon la revendication 1, comprenant une pluralité de clefs disposées en différents endroits des pistes d'enregistrement, les clefs étant adaptées pour être utilisées avec un logiciel destiné à détecter la présence des clefs par une distribution de données aléatoires générées par lesdits clefs, le logiciel étant en plus adapté pour effacer au moins une clef, à chaque fois que le programme est utilisé, les clefs agissant ainsi comme des "laissez-passer" permettant au programme d'être

utilisé seulement un nombre de fois prédéterminé.

7. Support magnétique de stockage d'informations selon la revendication 1, dans lequel ledit substrat est un disque souple.

8. Procédé pour produire un support magnétique souple de stockage d'informations ayant une signature magnétique incopiable caractérisé en ce que l'on enregistre au moins une clef sur une piste d'enregistrement du support, la clef étant composée pour partie de transitions différentes de celles utilisées pour le reste des informations et comprenant une suite de codes hors-norme qui ne peuvent être récupérés par un circuit de récupération de données, lesdites transitions différentes fournissant des données aléatoires lors de la lecture de la clef au moyen dudit circuit.

9. Procédé selon la revendication 8, dans lequel la clef est obtenue en modifiant la fréquence d'horloge usuelle.

10. Procédé selon la revendication 8, dans lequel la clef est réalisée en générant un signal d'effacement obtenu par un courant continu.

11. Procédé selon la revendication 8 comprenant en plus un numéro de série qui est enregistré après la clef pour l'identification du support.

30

35

40

45

50

55

60

65

6

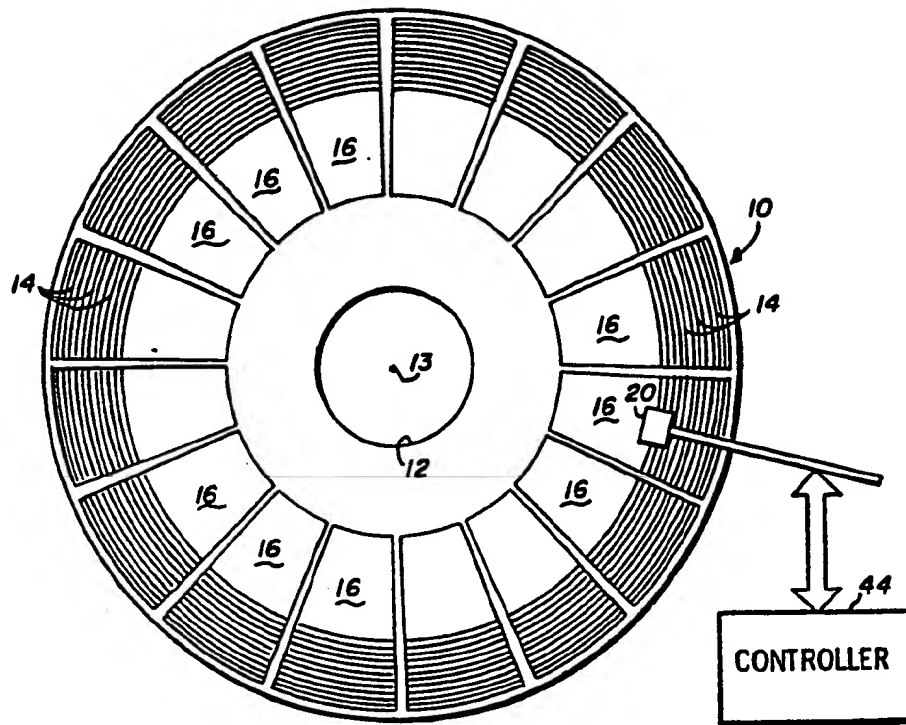


Fig. 1

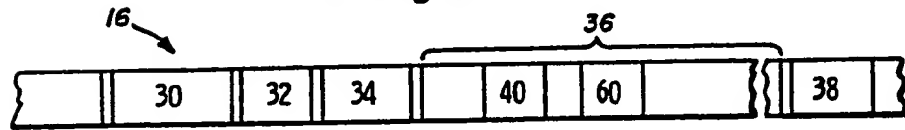


Fig. 2

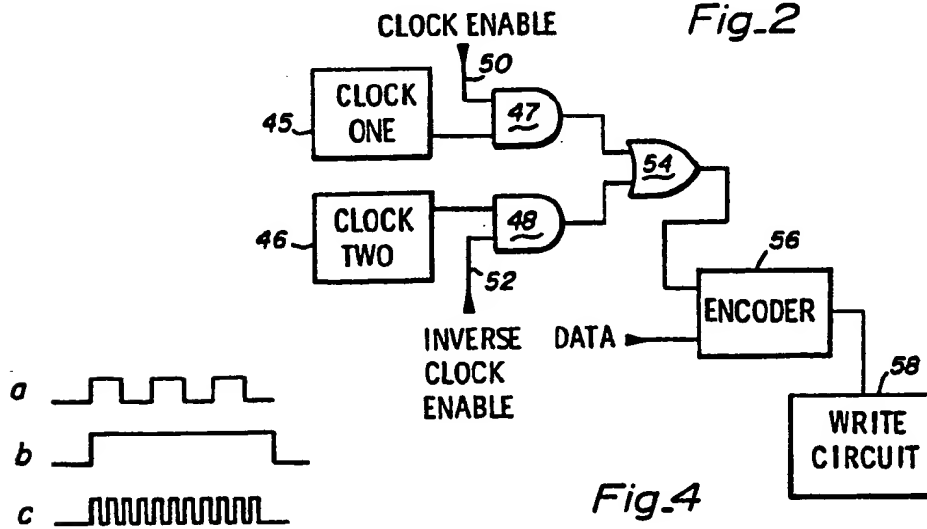


Fig. 3